White Paper

Understanding the McAfee Endpoint Security 10 Threat Prevention Module

Key enhancements and new capabilities

Table of Contents

This white paper is for security administrators responsible for managing McAfee® Endpoint Security Solutions. It covers the Threat Prevention module of McAfee Endpoint Security, which replaces the McAfee VirusScan® Enterprise 8.8 product. Intel Security has made significant improvements in this new module. There are several new capabilities introduced in the Threat Prevention module that are different from or not available in the McAfee VirusScan Enterprise product. This white paper provides you with an understanding of new capabilities and highlights the differences between McAfee VirusScan Enterprise 8.8 and McAfee Endpoint Security 10.

McAfee Anti-Malware Engine Core

Key benefit: Better scanning performance

The capacity and capabilities of endpoints have increased dramatically in the past several years, and multiterabyte endpoints are now the norm in the enterprise. Previous generations of antivirus solutions, which scanned every individual file, are not optimized for this type of environment. To better address the needs of this type of environment with speed and efficiency, the McAfee Endpoint Security Framework Anti-Malware Engine Core (McAfee AMCore)—the anti-malware scanning technology of the Threat Prevention module—provides enhanced capabilities to address the requirements of these large environments and counter emerging and advanced malware threats with speed and efficacy.

McAfee AMCore intelligently scans only items that really need to be scanned, instead of scanning all items equally. It accomplishes this efficiently without requiring you to make any configuration changes in the product. This technology is proven in performance and is running on millions of consumer endpoints. McAfee AMCore has also been subjected to numerous efficacy and performance tests by third-party organizations, such as AV-TEST.org and AV-Comparatives.org. As with the previous anti-malware engine, each release of McAfee AMCore content undergoes extensive quality and safety testing.

Zero-Impact Scanning

Key benefits: Increased performance and scanning that is invisible to users

What is it?

Scanning, especially on-demand full scans, can be resource-intensive. Zero-impact scanning is an on-demand capability that runs only when a system is idle and when users are not on their computers.

How does it work?

McAfee Endpoint Security 10 monitors the system for idle states by watching disk utilization, user idle state, and full-screen mode (presentation mode). Here are the ways that each of these looks for idle status:

- Microsoft Windows Management Instrumentation (WMI) performs checks at regular intervals to monitor disk usage. If disk usage over that time is less or more than the threshold limit, a notification is sent, and McAfee Endpoint Security 10 performs a deeper evaluation to determine the idle state.
- The “user idle” state is a derived value based on keyboard events, mouse movement, and full-screen mode.

- Full-screen mode is detected if the current application is run in full-screen mode, such as Microsoft PowerPoint presentations and videos playing in full screen mode.

The Threat Prevention module starts scanning within three minutes of determining an idle state based on the above factors. A running scan will pause automatically when users start using their systems or disk utilization increases. Scans resume at the next detected idle state where they left off. A system reboot will not terminate the scan.

Configuring zero-impact scanning
In McAfee® ePolicy Orchestrator® (McAfee ePO™) software, navigate to the "Policy Catalog > Endpoint Security Threat Prevention > On-Demand Scan." Under "Scheduled Scan Options," there is an option labeled "Scan only when the system is idle" for both full scans and quick scans. This will be enabled by default; however, scans (frequency, start time, and other factors) will still need to be scheduled using Client Task assignments.

Traditional On-Demand Scans—Scan Anytime Option

The Threat Prevention module supports traditional scans that start based on the schedule set by administrators. Scans will run until they are complete—without waiting for the idle condition. Administrators can also configure the user message, duration of the message, and the maximum number of times a user can postpone the scan by one hour.

Please note that on-demand scans can be configured to run anytime or only when the system is idle. Both scan types require a schedule and frequency.

Here is an example of anytime scanning and idle-time scanning for a full scan scheduled to start weekly on Mondays at 10 am.

- The full scan starts at 10 am. However, if the user is active on the system, the full scan pauses immediately and waits for the system to become idle before it resumes. The scan continues pausing and resuming until the full scan for that week is complete.

- When the "Scan Anytime" option is selected, the full scan starts at 10 am and continues to run until it finishes (as it does in McAfee VirusScan Enterprise 8.8).

It is recommended that the "Scan only when the system is idle" option be used for desktops and laptops because these systems are typically idle at some intervals during the day. "Scan anytime" is best suited for servers, as they don't typically enter an idle state.

Exploit Prevention Technology

Key benefit: Increased protection
The Threat Prevention module in McAfee Endpoint Security 10 provides a content-based Exploit Prevention capability. This capability replaces McAfee VirusScan Enterprise 8.8's buffer overflow protection and provides a broader range of coverage against vulnerabilities and exploits. Exploit Prevention content is updated monthly, based on research done by Intel Security's dedicated malware research team. The content is published in line with the Microsoft Black Tuesday vulnerability announcements. This content not only provides protection against zero-day exploits, but also offers some flexibility in the way that Microsoft patches can be applied.

Exploit Prevention includes the technologies listed below.

Generic buffer overflow protection (GBOP)
GBOP provides content-driven protection for a specific list of application programming interfaces (APIs) against one of the most notorious forms of attack. Buffer overflow attacks rely on programmer mistakes that occur when dealing with memory space for variables.

Data execution prevention (DEP)

DEP is a Microsoft Windows operating system security feature designed to prevent damage from viruses and other security threats by monitoring programs to ensure that they use system memory safely. Because it is enforced by the operating system, this protection provides an increase in performance and API coverage. Exploit Prevention will report if and when DEP is triggered.

Kevlar

Kevlar is a kill-bit security feature for web browsers and other applications that use ActiveX controls. A kill bit specifies the object class identifier (CLSID) of ActiveX controls identified as security vulnerability threats. This protection is also content-driven.

Suspicious caller

Suspicious caller protection detects code injected by an attacker that is running in memory. These exploits attempt to bypass traditional security protection mechanisms such as GBOP and DEP. Suspicious caller will also prevent return-oriented programming-based attacks.

Configuring Exploit Prevention

In McAfee ePO software, Exploit Prevention is found under: “Policy Catalog > Endpoint Security Threat Prevention > Exploit Prevention.” There are two protection levels: standard and maximum. Standard is the recommended default option. Increasing the protection level to maximum requires policy tuning and testing.

Enhanced Access Protection

Key benefits: Flexible configuration and ease of use

Access Protection (AP) capabilities in the Threat Prevention module have been enhanced to provide more flexibility to security administrators over those available in McAfee VirusScan Enterprise 8.8. These enhancements include the ability to:

- Specify more file and registry operations (such as read, write, create, delete).
- Create a single AP rule to protect files and registry entries instead of protecting only one per rule.
- Include or exclude processes at the rule level, based on file path, MD5, and digital signer, rather than simply based on file path.
- Create global exclusions that apply to all AP rules.

In addition, AP now proactively excludes all McAfee/Intel Security-signed processes from being subject to access controls. McAfee VirusScan Enterprise 8.8 does not support this capability.

Integration of Additional Modules

Key benefit: Reduced overhead of deploying and maintaining multiple products

McAfee Endpoint Security 10 uses an integrated client. In addition to Threat Prevention, it includes the Firewall module (previously McAfee Host Intrusion Prevention Firewall) and the Web Control module (previously McAfee SiteAdvisor® Enterprise). All three modules are integrated into a single McAfee Endpoint Security 10 client interface. Intel Security has maintained the flexibility for administrators to pick and choose which modules to deploy on endpoint systems. Although each module is designed to work independently, they leverage common components, such as self-protection, client interface, scheduler, and logging, to provide a better overall user experience when managing these products. To learn more about McAfee Host Intrusion Prevention Firewall and SiteAdvisor Enterprise, please refer to McAfee Endpoint Security 10 online help to gain an understanding of the capabilities of the Firewall and Web Control modules.

Policy configurations

Although the McAfee ePO software extensions for each module remain separate, we have grouped them into a single package (called McAfee Endpoint Security) in the McAfee ePO Software Manager. In McAfee ePO server, there will be four extensions available:

- McAfee Endpoint Security Threat Prevention
- McAfee Endpoint Security Firewall
- McAfee Endpoint Security Web Control
- McAfee Endpoint Security Platform (also called Common)

While the Threat Prevention, Firewall, and Web Control extensions include their respective configuration options, Common includes configuration options that are shared by all modules. These options include Self-Protection, McAfee Endpoint Security client interface, scheduler, and logging. Please note the configuration for the McAfee Agent remains separate.

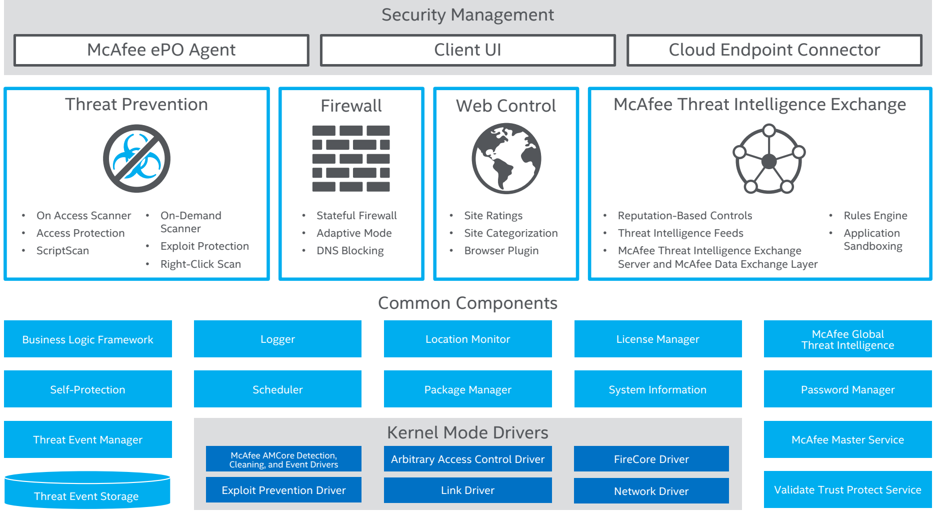


Figure 1. The McAfee Endpoint Security 10 platform.

Client packages for modules

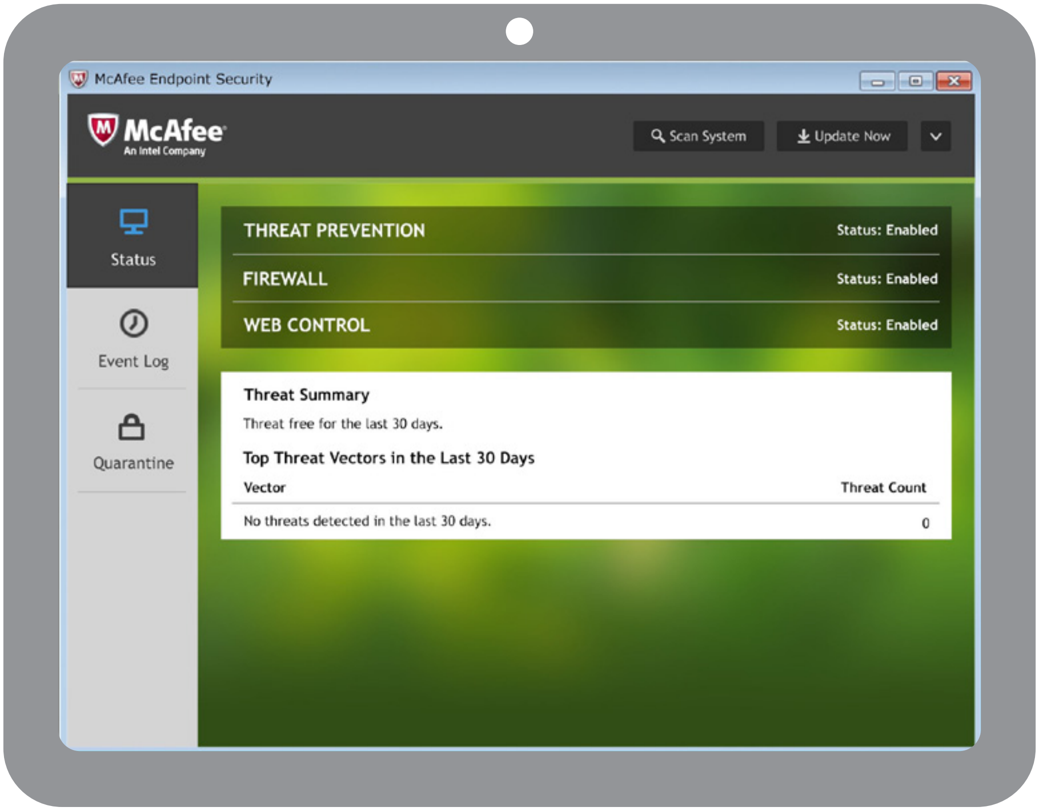
The client deployment package for each module is separate. Whether McAfee ePO software or a third-party tool is used to deploy the client package, the client package to deploy on the endpoints can be selected using the installer that is shared by all modules for a consistent installation experience.

Integrated dashboards

There are several dashboards in McAfee ePO software that are designed to provide an integrated view of the McAfee Endpoint Security 10 modules. For example, the "McAfee Endpoint Security: Installation Status" dashboard provides a view of all McAfee Endpoint Security 10 modules that are installed on the endpoint systems. To learn more about all of the dashboards that are available, please refer to online help.

Client User Interface

The McAfee Endpoint Security 10 client interface is modern, touch-friendly, and designed to address the needs of users, help desk administrators, and McAfee ePO software administrators. The client is also modular—only the modules that are installed on the client appear in the interface.



THREAT PREVENTION	Status: Enabled
FIREWALL	Status: Enabled
WEB CONTROL	Status: Enabled

Threat Summary

Threat free for the last 30 days.

Top Threat Vectors in the Last 30 Days

Vector	Threat Count
No threats detected in the last 30 days.	0

Figure 2. The McAfee Endpoint Security 10 user interface is highly intuitive, easy to navigate, and features support for touch screens.

The client supports three modes of operation:

- **Standard access:** This is the default configuration of the client user interface for McAfee ePO-managed systems. In this mode, users don't have access to any configurations (policy settings), but they do have the ability to perform basic functions, such as initiating on-demand scans, viewing the quarantine folder, accessing log files, and getting new updates. This mode also supports password-based administrator access. Once the password has been entered, the client allows access to all configuration settings. This ability is useful to help desk administrators who might require access to policy settings in troubleshooting scenarios. Please note that any changes made to policy settings locally will be overwritten as soon as the client receives a policy update from McAfee ePO software.
- **Full access:** This mode allows full access to the client interface, including the ability to view and edit policy settings without the need to enter a password. This mode is designed mainly for stand-alone (unmanaged or self-managed) systems.
- **Lock client interface:** This mode completely hides the client user interface from users.

Additional Improvements

Automatic scanning of files downloaded from the web

The Web Control and Threat Prevention modules work together to provide enhanced protection and visibility of files downloaded from the web. Please note that both Web Control and Threat Prevention must be installed on the endpoint system to use this feature.

Configuring file download protection

In McAfee ePO software, navigate to “Policy Catalog > Endpoint Security Web Control > Options.” Under “Action Enforcement,” the “Enable file scanning for file downloads” option will be available and will be enabled by default. The McAfee Global Threat Intelligence (McAfee GTI) sensitivity levels can also be set specifically for scanning downloaded files. McAfee GTI settings for these scans override and are independent of the McAfee GTI sensitivity setting for on-access scan (OAS) and on-demand scan (ODS). For example, McAfee GTI sensitivity could be set to “Medium” for OAS and ODS and “High” for files downloaded from the web for an added level of protection. The source URL for these types of events can be captured for even stronger visibility into URLs that are malicious in nature.

On-demand scan configurations

The Threat Prevention module supports four different types of on-demand scan: full scan, quick scan, custom scan, and right-click scan. All scans can be configured by administrators and are much more flexible when compared to McAfee VirusScan Enterprise 8.8. For example:

- Full scan and quick scan are configured through policies instead of the client task catalog.
- Full scan, quick scan, and custom scan can be configured to run only when the system idle, as described earlier.
- Right-click scan is completely configurable through a policy.

Password protection for uninstallation

All modules, including the Threat Prevention module, can be password-protected from being uninstalled. Even local administrators of a system won’t be able to uninstall modules without the password for this operation.

Content rollback in McAfee ePO software

The Threat Prevention module allows rollback of McAfee AMCore content using a client task in McAfee ePO software, providing administrators with more flexibility.

Enhanced logging, threat events, and reporting

The Threat Prevention module provides three distinct types of logs and event reporting accessible from the client interface:

- **Activity logs:** These logs are designed to capture information-only events. They include events, such as when system idle state was determined, when a scan started, paused, or resumed, and which files couldn’t be scanned.
- **Threat events:** These are more descriptive in the Threat Prevention than in McAfee VirusScan Enterprise and include attributes that provide visibility into host name and location, detection feature, file hash, file date and time, if detection occurred through .DATs or McAfee GTI lookup, and duration of the file on system before it was detected. Natural language descriptions are used for threat events, with information available in both the client interface and McAfee ePO software.

Here is an example event:
Username\name ran C:\Program Files (x86)\Internet Explorer\iexplore.exe, which attempted to access :\Users\username\AppData\Local\Microsoft\Windows\INetCache\IE\1WPY3AJV\jZipSetup-r427-n-bi (1).exe.50l18x8.partial and the threat potentially unwanted program SearchSuite was detected and deleted.

- **Debug logs:** These are the standard troubleshooting logs that, when enabled, generate detailed information that can be consumed by Intel Security Technical Support to help troubleshoot issues.

Common policies for Windows and Mac systems

Both Windows and Macintosh systems can now be managed by the same policy configurations in McAfee ePO software. Administrators no longer need to manage Threat Prevention policies for the Mac platform separately.

Improved scanning for Internet Explorer (IE)

ScriptScan is a browser helper object that intercepts scripts run by IE and scans both JavaScript and vbscript for malicious activity. It has been improved to deliver better performance and compatibility. It only scans scripts for Internet Explorer; it does not change registry entries for JavaScript or vbscript. Instead, a browser helper object is used to determine the URLs that are being visited and to hook the APIs needed to intercept scripts.

Migration assistant

The Threat Prevention module supports migration of McAfee VirusScan Enterprise 8.8 policies. Please refer to the Migration Guide for details on how existing McAfee VirusScan Enterprise 8.8 policies and client configurations can be migrated.

Changes from VirusScan Enterprise 8.8

The purpose of this section is to highlight features, processes, and workflows that are different in the Threat Prevention module versus VirusScan Enterprise 8.8.

Policy configurations

- The Threat Prevention module no longer supports the “Workstation Only” and “Server Only” concept that existed in the McAfee VirusScan Enterprise 8.8 extension policies. Separate policies for workstations and servers may be required. Please refer to the Migration Guide to understand how existing McAfee VirusScan Enterprise 8.8 configurations are related and how they will be handled during migration.
- To simplify policy configuration in Threat Prevention, the number of policy categories has been reduced. For example, “High-Risk,” “Low-Risk,” and “Normal” on-access scan policies are combined into a single policy category.
- Instead of the McAfee VirusScan Enterprise targeted scan, out-of-the-box polices for full scan and quick scan are supported.
- The Access Protection categories concept has been eliminated. Access Protection rules now exist as a flat list of items. Self-Protection (protection of McAfee/Intel Security resources) has also been decoupled from Access Protection. Self-Protection is now part of the McAfee Endpoint Security platform in the “Options” policy.
- The port blocking rules that existed in McAfee VirusScan Enterprise have been permanently removed from Threat Prevention. You can leverage the Firewall module for port blocking capabilities.
- Considerations for exclusions:
  - To exclude files from a scan because there are local or custom applications that could trigger detections, exclusions must be defined.

  - File exclusions were previously used to help improve performance. The trust models in McAfee AMCore and the use of caching and file exclusions in this way might be counterproductive.
  - To exclude files from scanning purely for performance reasons, process exclusion is the most effective approach. Please refer to the McAfee AMCore Trust Model document for further details on the McAfee AMCore scanning mechanism.
- **"Let McAfee Decide":** When you let McAfee/Intel Security decide whether a file requires scanning, the on-access scanner uses trust logic to optimize scanning. Trust logic improves security and boosts performance by avoiding unnecessary scans. For example, it analyzes and considers some programs to be trustworthy. If it verifies that these programs haven't been tampered with, the scanner might perform reduced or optimized scanning. Please refer to the McAfee AMCore Trust Model document for further details on the McAfee AMCore scanning mechanism.

Content

- The traditional McAfee VirusScan Enterprise content (signatures or .DATs) in the Threat Prevention module are referred to as V3 .DATs by McAfee Labs. V3 .DATs have a different structure, with enhanced capabilities, compared to McAfee VirusScan Enterprise .DATs. The McAfee Endpoint Security 10 client and McAfee ePO software refer to these .DATs as "McAfee AMCore content."
- Engine updates in the Threat Prevention module are now bundled with the .DATs in the content by Intel Security to ensure the right combination of components. V3 .DATs with the new engine are thoroughly tested by McAfee Labs before release, and deployment is throttled. This entire process is seamless and handled automatically.
- Exploit Prevention content is a separate content stream and is released monthly. The McAfee Endpoint Security 10 client and McAfee ePO software refer to this content as "Exploit Prevention content." This content doesn't support the roll-back capability available with the V3 .DATs.

McAfee Endpoint Security 10 Client Interface

- The McAfee Endpoint Security 10 client interface supports password-based unlocking. When the client interface is unlocked, settings and configuration for all the McAfee Endpoint Security 10 modules that are installed on the system are visible. Further granularity to lock and unlock only certain areas of the client interface is not available at this time.
- The "About" box displays installed modules, versions, and management mode, as well as McAfee AMCore and Exploit Prevention content versions.
- The client interface can be accessed by right-clicking the McAfee icon in the Windows system tray.

Learn More

Have questions? Looking for more information on how McAfee Endpoint Security 10 works? Visit the McAfee Endpoint Security 10 page and Intel Security Community page.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com